Ne répondez pas aux questions par un simple *oui* ou *non*. Argumentez vos réponses, prouvez vos affirmations. Les étoiles marquent les exercices difficiles : réservez-les pour la fin.

Documents autorisés. Pas de calculettes. Pas d'ordinateur. Pas de téléphone.

IMPORTANT : Notez le numéro de sujet sur votre copie.

Question 1

On considère le chiffrement par permutation avec pour clef la permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix}.$$

(a) Encodez le message « AUTOTRESVASYVASYMENT ».

(b) Décodez le message « AMCPPUSLNIRVEASMAYRS ».

(c) $(*)$ On a vu en cours que le chiffrement par permutation est un cas particulier du chiffrement de Hill. Donnez les matrices d'encodage et décodage qui correspondent à la clef ci-dessus.

Question 2

On veut transmettre un message sur un canal bruité. Pour cela, on commence par encoder les lettres de l'alphabet sur 5 bits par l'écriture en base 2 de leur position : $A = 00001$, $B = 00010$, etc.

(a) Encodez le message « BLEU »

Ensuite, pour permettre la correction d'erreurs, on applique lettre par lettre le code linéaire de paramètres $[9, 5, 3]$ défini par la matrice de parité

$$H = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

(b) Calculez la matrice génératrice du code.

(c) $(*)$ Exhibez deux mots de code à distance 3 l'un de l'autre.

(d) Combien d'erreurs au plus peut corriger ce code ?

(e) Encodez le message de la question (a).

(f) Décodez le message « 100110111 000110111 011010011 011011010 ».

Question 3

Alice et Bob veulent convenir d'un secret en utilisant le protocole d'échange de clef de Diffie-Hellman. Ils se mettent d'accord pour le corps $\mathbb{Z}/29\mathbb{Z}$ et pour le générateur $g = 8$. Alice choisit la clef secrète $a = 22$ et Bob $b = 26$.

(a) Calculez les clefs publiques de Alice et Bob.

(b) Calculez la clef partagée.

Utilisez l'algorithme d'exponentiation binaire pour répondre aux deux questions. Ne donnez pas seulement les résultats finaux : développez en détail les étapes du calcul. Pour vous aider dans le calcul, la table de multiplication de $\mathbb{Z}/29\mathbb{Z}$ est donnée en annexe.

(c) $(*)$ Calculez $17^{403} \bmod 29$.

Question 4

(a) (∗) À l'aide du théorème des restes chinois, calculez l'inverse de 53 modulo 72.

On fixe le module RSA $N = 91 = 7 \cdot 13$.

(b) Calculez $\phi(N)$.

(c) Générez une clef publique e et une clef privée d non triviales (i.e., pas égales à 1 ou $\phi(N) - 1$), telles que

$$m^{ed} = m \mod N$$

pour tout $m \in \mathbb{Z}/N\mathbb{Z}$.

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
2	0	2	4	6	8	10	12	14	16	18	20	22	24	26	28	1	3	5	7	9	11	13	15	17	19	21	23	25	27
3	0	3	6	9	12	15	18	21	24	27	1	4	7	10	13	16	19	22	25	28	2	5	8	11	14	17	20	23	26
4	0	4	8	12	16	20	24	28	3	7	11	15	19	23	27	2	6	10	14	18	22	26	1	5	9	13	17	21	25
5	0	5	10	15	20	25	1	6	11	16	21	26	2	7	12	17	22	27	3	8	13	18	23	28	4	9	14	19	24
6	0	6	12	18	24	1	7	13	19	25	2	8	14	20	26	3	9	15	21	27	4	10	16	22	28	5	11	17	23
7	0	7	14	21	28	6	13	20	27	5	12	19	26	4	11	18	25	3	10	17	24	2	9	16	23	1	8	15	22
8	0	8	16	24	3	11	19	27	6	14	22	1	9	17	25	4	12	20	28	7	15	23	2	10	18	26	5	13	21
9	0	9	18	27	7	16	25	5	14	23	3	12	21	1	10	19	28	8	17	26	6	15	24	4	13	22	2	11	20
10	0	10	20	1	11	21	2	12	22	3	13	23	4	14	24	5	15	25	6	16	26	7	17	27	8	18	28	9	19
11	0	11	22	4	15	26	8	19	1	12	23	5	16	27	9	20	2	13	24	6	17	28	10	21	3	14	25	7	18
12	0	12	24	7	19	2	14	26	9	21	4	16	28	11	23	6	18	1	13	25	8	20	3	15	27	10	22	5	17
13	0	13	26	10	23	7	20	4	17	1	14	27	11	24	8	21	5	18	2	15	28	12	25	9	22	6	19	3	16
14	0	14	28	13	27	12	26	11	25	10	24	9	23	8	22	7	21	6	20	5	19	4	18	3	17	2	16	1	15
15	0	15	1	16	2	17	3	18	4	19	5	20	6	21	7	22	8	23	9	24	10	25	11	26	12	27	13	28	14
16	0	16	3	19	6	22	9	25	12	28	15	2	18	5	21	8	24	11	27	14	1	17	4	20	7	23	10	26	13
17	0	17	5	22	10	27	15	3	20	8	25	13	1	18	6	23	11	28	16	4	21	9	26	14	2	19	7	24	12
18	0	18	7	25	14	3	21	10	28	17	6	24	13	2	20	9	27	16	5	23	12	1	19	8	26	15	4	22	11
19	0	19	9	28	18	8	27	17	7	26	16	6	25	15	5	24	14	4	23	13	3	22	12	2	21	11	1	20	10
20	0	20	11	2	22	13	4	24	15	6	26	17	8	28	19	10	1	21	12	3	23	14	5	25	16	7	27	18	9
21	0	21	13	5	26	18	10	2	23	15	7	28	20	12	4	25	17	9	1	22	14	6	27	19	11	3	24	16	8
22	0	22	15	8	1	23	16	9	2	24	17	10	3	25	18	11	4	26	19	12	5	27	20	13	6	28	21	14	7
23	0	23	17	11	5	28	22	16	10	4	27	21	15	9	3	26	20	14	8	2	25	19	13	7	1	24	18	12	6
24	0	24	19	14	9	4	28	23	18	13	8	3	27	22	17	12	7	2	26	21	16	11	6	1	25	20	15	10	5
25	0	25	21	17	13	9	5	1	26	22	18	14	10	6	2	27	23	19	15	11	7	3	28	24	20	16	12	8	4
26	0	26	23	20	17	14	11	8	5	2	28	25	22	19	16	13	10	7	4	1	27	24	21	18	15	12	9	6	3
27	0	27	25	23	21	19	17	15	13	11	9	7	5	3	1	28	26	24	22	20	18	16	14	12	10	8	6	4	2
28	0	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1

Table de multiplication de $\mathbb{Z}/29\mathbb{Z}$

Solutions

Solution 1

(a) On découpe le message en blocs de longueur 5

AUTOT RESVA SYVAS YMENT,

on applique la permutation σ à chaque bloc

UTAOT ESRVA YVSAS MEYNT,

et on recolle le tout

UTAOTESRVAYVSASMEYNT.

(b) On calcule la permutation inverse

$$\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 4 & 5 \end{pmatrix}$$

et on procède comme au point précédent, ce qui donne le message

CAMPPLUSNIERVASYMARS.

(c) À toute permutation $\sigma \in \mathcal{S}_n$ on peut associer une *matrice de permutation* $n \times n$. C'est la matrice qui agit sur les vecteurs à n coordonnées de la même façon que σ. Elle contient exactement un 1 par ligne et par colonne, toutes les autres entrées valent 0. À la i-ème ligne, le 1 apparaît à la colonne $\sigma(i)$.

Dans notre cas, la matrice de permutation est

$$P = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

On vérifie aisément que son action est compatible avec σ :

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 2 \\ 3 \\ 4 \\ 5 \end{pmatrix} = \begin{pmatrix} 2 \\ 3 \\ 1 \\ 4 \\ 5 \end{pmatrix}.$$

La matrice inverse de P peut être calculée à partir de σ^{-1}. Alternativement, nous savons que l'inverse de toute matrice de permutation est donnée par sa transposée, d'où :

$$P^{-1} = P^T = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Solution 2

(a) En appliquant lettre par lettre le codage, on a

00010 01100 00101 10101.

(b) La matrice génératrice du code est

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

(c) Le mot 000000000 appartient certainement au code, il suffit donc de trouver un autre mot contenant trois 1. Nous cherchons alors une combinaison de colonnes de G donnant un tel mot. En prenant, par exemple, la somme des trois premières colonnes on obtient

$$100000011 + 010001110 + 001001101 = 111000000.$$

Donc 000000000 et 111000000 sont deux mots de code à distance 3.

(d) La distance minimale du code est 3, donc le code peut corriger au plus $(3-1)/2 = 1$ erreur.

(e) Pour encoder le message précédent, il suffit de le multiplier lettre par lettre par la matrice G. Cela donne

$$000101011\ 011000011\ 001011010\ 101011001.$$

(f) On commence par calculer les quatre syndromes en multipliant chaque mot par la matrice H, cela nous donne

$$1000, \quad 1011, \quad 0111, \quad 1110.$$

En cherchant l'indice auquel les syndromes apparaissent dans H, on obtient les pattern d'erreur suivants

$$000001000\ 000100000\ 000010000\ 010000000,$$

qui, additionnés aux mots reçus, donnent les mots de code

$$100111111\ 000010111\ 011000011\ 001011010.$$

Il ne reste plus qu'à trouver le message correspondant à chaque mot de code, ce qui se lit dans les cinq premières coordonnées :

$$10011\ 00001\ 01100\ 00101.$$

Enfin, en inversant le codage du premier point, on obtient le message « SALE ».

Solution 3

(a) Les clefs publiques de Alice et Bob sont, respectivement, g^a et g^b. On commence par convertir les exposants en base 2 :

$$a = (10110)_2, \quad b = (11010)_2.$$

Sur la diagonale de la table de multiplication, on trouve les carrés successifs de g modulo 29 :

$$8^2 = 6, \quad 6^2 = 7, \quad 7^2 = 20, \quad 20^2 = 23.$$

Ensuite on multiplie ensemble les éléments qui correspondent aux 1 dans l'expansion binaire de a et b :

$$g^a = 6 \cdot 7 \cdot 23 = 9, \quad g^b = 6 \cdot 20 \cdot 23 = 5,$$

(b) La clef partagée est $(g^a)^b = (g^b)^a = g^{ab}$. Pour avoir le moins d'opérations à calculer, on utilise le petit théorème de Fermat : on sait que

$$g^{ab} = g^{ab \bmod p-1} = g^{572 \bmod 28} = g^{12};$$

on écrit 12 en base 2, ce qui donne $(1100)_2$; et on conclut

$$g^{ab} = 7 \cdot 20 = 24.$$

(c) On sait que l'ordre de tout élément de $\mathbb{Z}/29\mathbb{Z}$ est au plus 28, on commence donc par calculer l'ordre de 17. Grâce à la table de multiplication on trouve rapidement que $17^4 = 1$, d'où on déduit

$$17^{403} = (17^4)^{100} \cdot 17^3 = 1 \cdot 17^3 = x^3.$$

Solution 4

(a) On sait que $72 = 9 \cdot 8$, le théorème des restes chinois nous permet donc de calculer l'inversion modulo 8 et modulo 9 et enfin de remonter le résultat modulo 72.

On commence par la réduction

$$53 = 5 \bmod 8, \qquad 53 = 8 \bmod 9.$$

L'inversion est maintenant immédiate et peut même être calculée de tête :

$$5^{-1} = 5 \bmod 8, \qquad 8^{-1} = 8 \bmod 9.$$

Nous cherchons maintenant un élément $c \in \mathbb{Z}/72\mathbb{Z}$ congru à $a = 5$ modulo 8 et à $b = 8$ modulo 9. La relation de Bezout entre 8 et 9 se calcule aussi de tête :

$$(-1) \cdot 8 + 9 = 1,$$

l'élément cherché est donc

$$c = b \cdot (-1) \cdot 8 + a \cdot 9 = -19.$$

(b) On a $\phi(N) = \phi(7 \cdot 13) = (7-1) \cdot (13-1) = 72$.

(c) Pour que $m^{ed} = m$ pour tout m, il faut que

$$ed \equiv 1 \mod \phi(N).$$

On peut alors prendre les éléments calculés au premier point : $e = 53$ et $d = -19$, par exemple.